REFUND CHECKS FROM FEDERAL TRADE COMMISSION – THEY'RE REAL

If you are a regular reader of this column, you've read about all manner of scams, frauds, and rip-offs, and probably wondered, "Do they ever catch those guys?" That's a question I get about every time I speak to a civic group. And the short answer is, once in a while the crooks are caught.

Here's the latest example, courtesy of Jeanne McClure of Clinton. She received a check paying her $26 and some change. The accompanying letter told her the check represented her share of a settlement in *FTC vs. Allstar Marketing Group.* The Federal Trade Commission (FTC) sued Allstar Marketing Group in federal court for over-billing customers. Allstar marketed consumer products through direct sales TV commercials, usually with a "buy one - get one free" offer.

Allstar settled the lawsuit, agreeing to pay 218,000 customers $7.2 million. Now, Jeanne doesn't remember buying anything like this, but the settlement noted these activities by Allstar went back to 1999. I know of a woman in Dewitt who received the same refund, so I suspect more are on the way. If you received such a check, it is good, this is a real deal, but you do need to cash the check within sixty days.

EMAIL FROM APPLE – IT'S A PHISHING SCAM

If you use email, you should know the risk of opening links which appear in emails from unfamiliar sources. Opening these links can open up your computer, or indeed, any network you use, to hacking. This is a favorite method of cyber-criminals around the world to penetrate networks. They call it "spear-phishing" or "phishing".

Since most email users know of this risk, cyber-criminals must devise clever ruses to trick us into opening their links. A Clinton woman reported one such clever ruse, which worked, at least partially.

The woman received an email appearing to come from the Apple ID Store, with the subject line "Purchases Receipt Spotify Music Premium Subscription". The email text appeared like a receipt, showing someone charged her "credit card" $23.99 for the subscription. Although the woman knew Spotify was a music subscription service, she knew she did not subscribe. A link embedded in the email told her, "If you did not make this purchase, open this link to cancel". The woman opened the link, which revealed a prompt asking for her Apple account information. Alarm bells started sounding at this point, and the woman closed out of the email. She contacted Apple, who denied they sent the email, and described it as phishing

As the woman wrote to me in an email, “these emails are most unsettling, because you think at first someone has hacked into your accounts or credit cards.” Which is exactly the response the crooks wanted, to provoke momentary alarm, leading their victim to an impulsive action.

This particular phishing email is drew a public warning from the Federal Trade Commission on 2/23/18, cautioning us about opening attachments, or providing usernames and passwords in such emails.

PHISHING TEXT MESSAGE PUSHES BITCOIN

I’m surprised it took as long as it did, but bitcoin finally showed up mentioned in a complaint I received. Laqueda Walker of Clinton reported she received a text message informing her “your debit card has been authorized to buy .5 DC.” The text went on to ask Laqueda to call a number if she did not authorize the transaction. Laqueda called. The man who answered told her someone charged her bank account $900 to buy bitcoin (or DC, meaning digital currency). When she disputed this, he wanted to refund the money to her bank account. To accomplish this, Laqueda needed to allow this man access to her computer and bank account. Well, she was not having anything to do with that, and hung up.

Just like the email I wrote about, this text message used the same kind of trick – alarm the victim into thinking someone used their debit or credit card, getting the victim to take some action.

Both the email and the text message phishing should warn us to be very suspicious of any communication coming out of the blue, which wants something from us. Before you act on something like this, always sit back, think about it, and talk to someone else about it.

DEFENSIVE DRIVING COURSE

Seniors vs. Crime, along with AARP and Clinton Community College, is sponsoring a defensive driving course this spring. This session is scheduled for May 8th, 2018, from 10 am to 3 pm, at the Technology Center at 1951 Manufacturing Drive. This is a classroom exercise, with a hot lunch furnished by Seniors vs. Crime.

To register, call 563-244-7100. Cost for AARP members is $15, for non-members is $20. The instruction will cover review safe driving, emphasizing how reactions and perceptions might change as we age.

CONTACT SENIORS VS. CRIME

Let me know about scams, fraud, or other crookedness you run across. Most of what I learn, I learn from you. Contact me at Seniors vs. Crime, Clinton County Sheriff's Office, 563-242-9211 extension 4433, or email me at randymeier@gapa911.us.

End of column/rmeier